UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,239	09/12/2003	David D. Brandt	03AB014A/ALBRP303USA	6849

7590 04/05/2007

Susan M. Donahue
Rockwell Automation
704-P, IP Department
1201 South 2nd Street
Milwaukee, WI 53204

EXAMINER	
PHAM, THOMAS K	
ART UNIT	PAPER NUMBER
2121	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/661,239	**Applicant(s)** BRANDT ET AL.	
	Examiner Thomas K. Pham	**Art Unit** 2121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Response to Amendment

1. This is in response to the request for re-consideration filed 12/22/2006.

2. Applicant's arguments with respect to claims 1-33 have been considered but are moot in view of the new ground(s) of rejection.

Quotations of U.S. Code Title 35

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim Rejections - 35 USC § 102

5. Claims 1, 5-7, 9, 10, 20, 23-25, and 27-29 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,421,571 ("Spriggs").

Regarding claim 1

Spriggs teaches the invention including an automation security system, comprising: an asset component that defines an industrial automation device (see C 3 L 20-24); an access component that defines one or more security attributes associated with the industrial automation device (see C 3 L 53-57); and a security component that regulates access to the industrial automation device based upon the security attribute (see C 27 L 65 to C 28 L 6).

Regarding claim 20

Spriggs teaches the invention including an automation security system, comprising: a server that manages a network interface between networked industrial automation devices and other devices attempting access to the networked industrial automation devices (see C 3 L 53-57); a security management module associated with the network interface that enforces an enterprise wide policy and that manages security threats directed to the networked industrial automation devices (see C 27 L 65 to C 28 L 6).

Regarding claim 24

Spriggs teaches the invention including an automation security methodology, comprising: electronically analyzing an industrial automation device (see C 3 L 20-24); programmatically modeling the industrial automation device in accordance with network security considerations (see C 3 L 53-57); and automatically developing a security framework for an automation system based in part on the modeling of the industrial automation device and a network access type (see C 27 L 65 to C 28 L 6).

Regarding claim 28

Spriggs teaches the invention including an automated security system for an automation control environment, comprising: means for defining one or more security attributes associated with at least one network request (see C 3 L 20-24); means for processing the one or more security attributes (see C 3 L 53-57); means for automatically determining which network devices require security resources (see C 3 L 45-52; means for controlling access to at least one of a network device and an industrial automation component based in part on the one or more security attributes (see C 27 L 65 to C 28 L 6).

Regarding claim 29

Spriggs teaches the invention including a security schema for a factory automation system, comprising: a first data field that describes industrial automation devices (see C 27 L 65-66); a second data field that describes security parameters for the industrial automation devices (see C 28 L 1-6); and a schema that associates the first and second data fields, the schema employed to limit access to the industrial automation devices based upon the security parameters (see C 27 L 66-67).

Regarding claim 5

Spriggs teaches the asset component describes at least one of factory components and groupings, the factory components are at least one of sensors, actuators, controllers, I/O modules, communications modules, and human-machine interface (HMI) devices (see C 3 L 45-52 and C 7 L 2-5).

Regarding claim 6

Spriggs teaches the groupings include factory components that are grouped into at least one of machines, machines grouped into lines, and lines grouped into facilities (see C 3 L 53-57).

Regarding claim 7

Spriggs teaches the groupings have associated severity attributes such as at least one of risk and security incident cost (see C 4 L 31-37).

Regarding claim 9

Spriggs teaches a set of generic IT components and specifies parameters to assemble and configure the IT components to achieve flexible access to the industrial automation device (see C 6 L 55-61).

Regarding claim 10

Spriggs teaches the IT components include at least one of switches with virtual local area network (VLAN) capability, routers with access list capability, firewalls, virtual private network (VPN) termination devices, intrusion detection systems, AAA servers, configuration tools, and monitoring tools (see C 7 L 26-44).

Regarding claim 23

Spriggs teaches at least one of: an authentication with the one or more servers to establish a secure link; a secure link to authenticate and authorize access to a requestor of the networked industrial automation device; and establishment of a secure session with the requestor if access is authorized (see C 3 L 45-52 and C 7 L 2-5).

Regarding claim 25

Spriggs teaches analyzing one or more security attributes to determine whether access should be granted to the one or more industrial automation assets (see C 3 L 20-25).

Regarding claim 27

Spriggs teaches at least one of: determining whether to grant access to the one or more automation assets; granting access from the industrial automation device; and granting access from the industrial automation device; and granting access from a network device associated with the industrial automation device (see C 27 L 65 to C 28 L 6).

Claim Rejections - 35 USC § 103

6. Claims 2-4, 11-19, 21, 22, 26, and 30-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spriggs in view of U.S. Patent Application Publication No. 2004/0034774 ("Le Saint").

Regarding claims 2-4, 26 and 30

Spriggs does not specificall discuss the one or more or more security attributes including at least one of a role attribute, a time attribute, a location attribute, and an access type attribute; the security component is based on at least one of a formal threat analysis, a vulnerability analysis, a factory topology mapping and an attack tree analysis; the security component is based on at least one of automation and process control security, cryptography, and Authentication/Authorization/Accounting (AAA).

However, Le Saint teaches the one or more or more security attributes including at least one of a role attribute, a time attribute, a location attribute, and an access type attribute (see paragraphs 6 and 10); the security component is based on at least one of a formal threat analysis, a vulnerability analysis, a factory topology mapping and an attack tree analysis (see paragraph 48); the security component is based on at least one of automation and process control security, cryptography, and Authentication/Authorization/Accounting (AAA) (see paragraph 13).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the security attributes and security component of Le Saint with the system of Spriggs because it would provide for the purpose of enforcing control aspect stated in the attributes including security policies and delegated privilege state.

Regarding claims 11-22 and 31-33

Spriggs does not specifically disclose security parameters and policies that are developed for physical and electronic security for various component types; at least one of security protection levels, identification entry capabilities, integrity algorithms, and privacy algorithms; the security component includes at least one of authentication software, virus detection, intrusion detection, authorization software, attack detection, protocol checker, and encryption software; at least one of acts as an intermediary between an access system and one or more automation components, and facilitates communications between the access system and the one or more automation components; the security attributes are specified as part of a network request to gain access to the one or more factory assets, the security attributes included in at least one of a group, set, subset, and class; the security component employs at least one authentication procedure and an authorization procedure to process the network request; one or more security protocols including at least one of Internet Protocol Security (IPSec), Kerberos, Diffie-Hellman exchange, Internet Key Exchange (IKE), digital certificate, pre-shared key, and encrypted password, to process the network request; at least one of an access key and a security switch to control network access to a device or network; the access key further comprises at least one of time, location, batch, process, program, calendar, GPS (Global Positioning Information) to specify local and wireless network locations, to control access to the device or network; the security management module at least one of schedules audits, establishes a security policy, applies the policy from a single or distributed console, and generates reports that identify potential weaknesses in security; the security management module provides an interface to at least one of add, delete and modify security rights of an individual, a group, or a device and distribute security information to various controllers and control devices; a response schema to provide status to a requesting network device; the response schema including at least one of a status field, a time field, an access type field, an access location field, and a key field, an attachment field to indicate other security data follows the response schema.

However, Le Saint teaches;

security parameters and policies that are developed for physical and electronic security for various component types (see paragraph 50);

at least one of security protection levels, identification entry capabilities, integrity algorithms, and privacy algorithms (see paragraph 50);

the security component includes at least one of authentication software, virus detection, intrusion detection, authorization software, attack detection, protocol checker, and encryption software (see paragraph 52);

at least one of the industrial automation devices acts as an intermediary between an access system and one or more automation components, and facilitates communications between the access system and the one or more automation components (see paragraph 52);

the security attributes are specified as part of a network request to gain access to the one or more factory assets, the security attributes included in at least one of a group, set, subset, and class; the security component employs at least one authentication procedure and an authorization procedure to process the network request (see paragraph 57);

one or more security protocols including at least one of Internet Protocol Security (IPSec), Kerberos, Diffie-Hellman exchange, Internet Key Exchange (IKE), digital certificate, pre-shared key, and encrypted password, to process the network request (see paragraph 54);

at least one of an access key and a security switch to control network access to a device or network; the access key further comprises at least one of time, location, batch, process, program, calendar, GPS (Global Positioning Information) to specify local and wireless network locations, to control access to the device or network (see paragraph 57);

the security management module at least one of schedules audits, establishes a security policy, applies the policy from a single or distributed console, and generates reports that identify potential weaknesses in security; the security management module provides an interface to at least one of add, delete and modify security rights of an individual, a group, or a device and distribute security information to various controllers and control devices (see paragraph 60);

a response schema to provide status to a requesting network device; the response schema including at least one of a status field, a time field, an access type field, an access location field, and a key field, an attachment field to indicate other security data follows the response schema (see paragraph 63).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the security system of Le Saint with the system of Spriggs because it would provide for the purpose of enforcing control aspect stated in the attributes including security policies and delegated privilege state.

7. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,421,571 ("Spriggs").

Regarding claim 8

Spriggs do not specifically teach an ISA S95 Model for Enterprise to Control System integration to integrate security aspects across or within respective groupings. "Official Notice" is taken that both the concept and advantages of providing an ISA S95 Model for Enterprise to Control System integration to integrate security aspects across or within respective groupings is well known and expected in the art. U.S. Patent Application Publication No. 2003/0014500 to Schleiss et al. discloses a preferred flow of communication between various process control and information technology systems are typically found within an enterprise defined by an ISA S95 model international standard (see paragraphs 7 and 8). It would have been obvious to one of ordinary skill in the art to include the ISA S95 model for Enterprise to Control system to Spriggs because it would provide for interacting between production or process control systems, enterprise resource planning systems and manufacturing execution systems to facilitate the integration of these systems.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner *Thomas Pham*; whose telephone number is (571) 272-3689, Monday - Friday from 7:30 AM - 4:00 PM EST or contact Supervisor *Mr. Anthony Knight* at (571) 272-3687.

Any response to this office action should be mailed to: **Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.** Responses may also be faxed to the **official fax number (571) 273-8300.**

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Thomas Pham
Primary Examiner

April 2, 2007